CONFERENCE PROCEEDINGS

U.S. GOVERNMENT WORKSHOP

BIOMETRIC STANDARDS IN SUPPORT OF THE GLOBAL WAR ON TERRORISM

25 MAY 2004

CO-SPONSORS

BIOMETRICS
DEPARTMENT OF DEFENSE
www.biometrics.dod.mil

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

EXECUTIVE SUMMARY

The need for technologies that can provide for better border security, force protection, and counterterrorism measures is essential to winning the Global War on Terrorism.

In the context of this war, it is increasingly important for U.S. Government agencies to have the capability to leverage biometric technology to link individuals to their previous names, aliases, and prior activities. Standards are critical to this effort's success because they enable interoperability among different systems that collect, store, and exchange biometric data. This interoperability is essential to sharing national security threat information with U.S. Government agencies and allies.

Recognizing this need, the Department of Defense (DoD) Biometrics Management Office (BMO), Department of Homeland Security (DHS), and the National Institute of Standards and Technology (NIST) co-sponsored the first U.S. Government Workshop on Biometric Standards in Support of the Global War on Terrorism on 25 May 2004. Workshop participants included 72 personnel representing 28 U.S. Government organizations. During the one-day workshop, these participants identified existing biometric standards, and gaps in current biometric standards development to satisfy their missions. Additionally, the participants developed strategies on how to leverage U.S. Government resources to continue biometric standards development at the national and international levels.

The DoD Deputy Chief Information Officer, Priscilla Guthrie, began the workshop by delivering the keynote address. A NIST representative presented an overview of biometric standards and their development through standards bodies. The Director, BMO, provided a DoD perspective on biometric standards in support of the Global War on Terrorism. Finally, a DHS representative provided an overview of DHS's experience with biometric standards.

During the workshop's afternoon session, participants engaged in two facilitated open discussions. A Transportation Security Administration (TSA) representative moderated the first open discussion, which focused on biometric applications, standards, and capability gaps. A NIST representative moderated the second discussion, which focused on biometric testing.

The following are the findings and conclusions that resulted from the workshop's activities:

- U.S. Government agencies should continue to work collaboratively to determine what specific biometric standards are needed. The stakeholders assuming responsibility for developing the standards must determine their near- and long-term strategies for implementation. From this perspective, the ultimate goal is the development of international standards to support the interoperability of multiple biometric technologies. However, national standards can often be developed more rapidly than international standards. Both national and international standards are under development. After approval of international standards, a graceful migration from national to international standards is expected (as long as the international standards meet the U.S. users' needs).

- There are currently no conformity assessment programs or conformance testing standards available to test or certify vendors' claims of conformity to biometric standards. Vendors' conformance to

standards is critical to government agencies successfully achieving interoperability. Efforts are underway to fill this gap. For example, U.S. Government agencies are participating in the drafting of the International Organization for Standardization (ISO) standard entitled, "BioAPI Conformance Testing—Part 1: Methods and Procedures." This conformance testing standard defines the methods and procedures for testing whether products conform to the BioAPI specification, a standard that enables biometric technologies to communicate with each other.

- Standards development must be accompanied by the development of policies that mandate the use of these standards.

TABLE OF CONTENTS

PROGRAM COMMITTEE

Department of Defense (Biometrics Management Office), John D. Woodward, Jr.

Department of Homeland Security (Transportation Security Administration), Rick Lazarick

Department of Homeland Security (United States Visitor and Immigrant Status Indicator Technology [US-VISIT] Program), Brad Wing

National Institute of Standards and Technology, Mike Hogan

National Institute of Standards and Technology, Fernando Podio

National Security Agency, Jeff Dunn

NOTE:

The Army Chief Information Officer/G-6, who represents the Secretary of the Army and is the DoD Executive Agent for Biometrics, provided invaluable support for this conference.

DISCLAIMER:

These Conference Proceedings do not represent an official policy of any U.S. Government organization.

COPIES OF CONFERENCE PROCEEDINGS:

To obtain an electronic copy of these Conference Proceedings, please visit www.biometrics.dod.mil.

PART I

MORNING SESSION

OPENING REMARKS

Presenter: Priscilla Guthrie, Deputy Assistant Secretary of Defense (Deputy Chief Information Officer)

The Department of Defense (DoD) recognizes that freedom and security are the central issues driving this U.S. Government Workshop on Biometric Standards in Support of the Global War on Terrorism. Further, DoD understands that leveraging biometric standards for our nation's defense is a collaborative effort. U.S. Government agencies must be able to openly collaborate on, and communicate information related to criminal and terrorist activities. The vision may be imagined as an Internet-like environment where information is easily shared with those who need it and are authorized to see it, whether across agencies or with our cooperating allies.

Biometric data is information that will be shared in this Internet-like environment and the DoD is increasing its collection effort of such data. In sharing this data, the DoD must prove the technologies involved work and are interoperable, thus a strong information assurance program must underpin data collection and distribution. Standards make the DoD's task possible because they facilitate interoperability and allow stakeholders to share information effectively.

This workshop was convened with the hope of answering the following questions:

- What do we collect, from a biometric perspective?
- What do we share?
- Who do we share it with?
- What national and international standards make biometric technology effective for us?

Through the participation of more than 70 personnel representing 28 U.S. Government organizations, this workshop is the first that aims to answer these basic questions. It is hoped there will be more workshops that focus on additional questions. Through this level of participation and a sustained effort, U.S. Government agencies will leverage their resources in order to make available the standards critical to implementing biometric technology in the Global War on Terrorism.

BIOMETRIC STANDARDS OVERVIEW

Presenter: Fernando Podio, Program Manager, National Institute of Standards and Technology (NIST)'s Biometric Standards Program, Computer Security Divisions, and Information Technology Laboratory (ITL)

NIST has been involved in developing biometric standards for decades. For example, with respect to biometric technology, NIST developed the standard entitled, "American National Standards Institute (ANSI)/NIST-ITL 1-2000, Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information." Widely used by national and international law enforcement communities, this biometric standard defines the content, format, and units of measurement for the exchange of fingerprint, palm print, facial/mug shot, and SMT full-image information that may be useful in identifying a subject.

Within the past five years, NIST has established strong collaborative relationships with biometric consortia that have allowed NIST to intensify its participation in biometric standards development. After the terrorist attacks on 11 September 2001, NIST believed the best strategy to accelerate the approval and adoption of biometric standards was to migrate most of the work to formal national and international bodies. To do so, NIST championed the successful establishment of national and international bodies for biometrics—the InterNational Committee for Information Technology Standards (INCITS) M1 and Joint Technical Committee 1 (JTC 1) Subcommittee 37 (SC37) Biometrics. Operating since January 2002, INCITS M1 is the primary standards body responsible for developing national biometric standards. Furthermore, INCITS M1 represents the United States within SC37, which is the international biometric standards body with 20 member countries. It is important to note that other standards bodies participate in various aspects of biometric standards development. For example, INCITS T4, the national standards body for information technology security, participates in the development of biometric security standards. SC27, the international counterpart to INCITS T4, participates in the development of international biometric security standards.

NIST Biometric Standards Program

The NIST Biometric Standards Program is based on a strategy to accelerate the development of biometric standards that government agencies have designated as high priority. To do so, NIST works in collaboration with government agencies, biometric standards incubators, and other biometric standards stakeholders. This strategy involves the following three components:

(1) Development of Standards to Meet User Requirements: The demand is high for a series of standards (e.g., interoperability, data interchange, performance, conformance) to be expeditiously developed and made available to support these user requirements.

(2) Pursuit of National Standards as well as International Standards: NIST's ultimate goal is the development of international standards to support high-performance interoperability systems. However, national standards can usually be developed more rapidly than international standards. To meet user

requirements in the near term, NIST encourages and pursues the development of national standards concurrently with the development of international standards. Over the long term, NIST plans for users (e.g., government agencies) to make the gradual migration from national to international standards once they are available, provided these international standards meet the users' needs.

(3) Collaboration with Industry and Users: NIST works to develop standards—whether at the national or international levels—rapidly. To do so, NIST supports the processing of consortia specifications that are technically sound and leverages the work of biometric standards incubators such as the U.S. Government Biometric Consortium and the National Biometric Security Project (NBSP). NIST also collaborates simultaneously with the biometric industry and users of the technologies to achieve a consensus on what standards are needed and on the content of these standards. NIST is working in close collaboration with other government agencies to develop the required standards (e.g., Department of Defense (DoD) Biometrics Management Office (BMO), Department of Homeland Security (DHS), intelligence community). An example of NIST's tactics is the participation and support of the development of the BioAPI specification (ANSI INCITS 358-2002) through consortia. This standard defines a generic way of interfacing with a broad range of biometric technologies. Its development began within the BioAPI Consortium, an entity comprised of more than 100 organizations. NIST is a member of the BioAPI Steering Committee. After the BioAPI Consortium approved the specification, it was proposed as an ANSI Fast Track candidate to INCITS. INCITS then worked to have the BioAPI specification established as an ANSI standard in 2002. After gaining ANSI status, INCITS M1 proposed the BioAPI specification as an international standard candidate. Another example of these tactics is the Common Biometric Exchange Formats Framework (CBEFF) (NIST Interagency Reports [NISTIR] 6529-A). The CBEFF specification is a U.S. Government standard spearheaded by NIST and the National Security Agency (NSA). Originally, it was published in 2001 as NISTIR 6529 and then revised and augmented by the NIST/ Biometric Consortium Biometric Working Group. NIST published the revised version as NISTIR 6529-A in April 2004 (available at www.nist.gov/biometrics). INCITS M1 also proposed this standard as an international standard candidate. It is currently undergoing development as an international standard within SC37.

NIST is also working to develop conformance testing standards that can be used to determine whether technology solutions appropriately meet the requirements defined in a standard. This is critical to system interoperability. To this end, NIST is (1) working with INCITS M1 and SC37 to develop conformance testing standards, (2) developing experimental conformance/system interoperability test beds (e.g., BioAPI, CBEFF) in support of the development of documentary standards, and (3) leading efforts to harmonize organizations' conformity assessment activities. Recently, NIST initiated efforts to educate INCITS M1 stakeholders on conformity assessments. These education efforts have included NIST conformity assessment experts (e.g., National Voluntary Laboratory Accreditation Program) briefing stakeholders, and proposing an INCITS M1 ad-hoc group to review issues on harmonizing conformity assessment with biometric standards. NIST also, in collaboration with NBSP, DoD BMO, Saflink, and the Biometric Foundation sponsored in INCITS M1 the development of a conformance testing methodology standard for ANSI 358-2002, the BioAPI specification.

Status of INCITS M1 and SC37 Standards Development

The following table outlines the status of standards under development within INCITS M1 and SC37.

BIOMETRIC DATA INTERCHANGE FORMATS	ANSI INCITS (APPROVAL TARGET DATES)	ISO / IEC (APPROVAL TARGET DATES)
Finger Minutiae Data Interchange Format—ANSI INCITS 378-2004	Approved 2004	1Q 2005
Finger Pattern Data Interchange Format—ANSI INCITS 377-2004	Approved 2004	1Q 2005
Face Image Data Interchange Format—ANSI INCITS 385-2004	Approved 2004	1Q 2005
Iris Image Data Interchange Format—ANSI INCITS 379-2004	Approved 2004	1Q 2005
Finger Image Data Interchange Format ANSI INCITS 381-2004	Approved 2004	2Q 2005
Signature/Sign Data Interchange Format	4Q 2004	4Q 2005
Hand Geometry Data Interchange Format	4Q 2004	4Q 2005
BIOMETRIC INTERFACE AND FORMATS FRAMEWORK	**ANSI INCITS (APPROVAL TARGET DATES)**	**ISO / IEC (APPROVAL TARGET DATES)**
BioAPI—Part 1: BioAPI Specification—ANSI INCITS 358-2002	Approved 1Q 2002	1Q 2005
CBEFF—Part 1: Data Element Specification	4Q 2004	1Q 2005
CBEFF—Part 2: Procedures for the Operation of the Registration Authority	Not Applicable	1Q 2005
BioAPI Conformance Testing—Part 1: Methods and Procedures	Not Applicable	4Q 2005
BIOMETRIC APPLICATION PROFILES	**ANSI INCITS**	**ISO / IEC**
Verification and Identification of Transportation Workers	3Q 2004	Not Applicable
Personal Identification for Border Management	3Q 2004	Not Applicable
Point of Sale Biometric Identification	1Q 2005	Not Applicable
DoD Implementation (new project)	2Q 2005	Not Applicable
Residential and Commercial Access Control	3Q 2005	Not Applicable
Employees	Not Applicable	4Q 2005

In summary, NIST is currently working to accelerate the development of biometric standards that government agencies have and will designate as high priority. To do so, NIST closely collaborates with other U.S. Government agencies (e.g., DoD BMO, NSA, intelligence community, DHS) and biometric standards incubators like the Biometric Consortium and the NBSP. NIST will use the opportunities that this workshop, and future ones, creates to assist U.S. Government agencies in first defining their user requirements and then leveraging their resources to establish standards to meet their requirements.

BIOMETRIC STANDARDS IN SUPPORT OF THE GLOBAL WAR ON TERRORISM: A DEPARTMENT OF DEFENSE PERSPECTIVE

Presenter: John D. Woodward, Jr., Director, Department of Defense (DoD) Biometrics Management Office (BMO)

On 27 December 2000, the Deputy Secretary of Defense formally established the DoD Biometrics Management Office (BMO) and its subordinate unit and technical arm, the Biometrics Fusion Center (BFC). The BMO is responsible for oversight of DoD biometric activities, planning and budgeting, policy and standards development, the acquisition process, DoD requirements gathering, public outreach, and the coordination of this work with other organizations. Currently, the BFC is working to establish itself as a biometric technology center of excellence for the DoD. The BFC performs test and evaluation of Commercial Off-The-Shelf (COTS) biometric technologies, supports the development of standards and performance measures, provides biometric repository support as required, and provides technical implementation and integration support to DoD organizations.

After the terrorist attacks of 11 September 2001, numerous government agencies expressed heightened interest in using biometric technology to improve security. This interest created the potential for the large deployment of multiple types of products using biometric technology. DoD considers interoperability to be one of its greatest needs to ensure the successful use of biometric technologies in the execution of its missions. To meet these needs, the BMO has made standards development one of its highest priorities because standards can ensure biometric interoperability across the DoD and the U.S. Government. The BMO's strategy for creating this interoperability is to:

- Develop biometric standards
- Coordinate standards development activities within the U.S. Government
- Test and evaluate biometric systems
- Implement standards

To accompany this strategy, the BMO is developing and advocating policy that mandates the use of biometric standards within DoD and is facilitating greater DoD and inter-agency coordination and cooperation.

The BMO executes its standards development strategy in multiple ways. First, the BMO coordinates and chairs the DoD BMO Biometric Standards Working Group. This group is comprised of DoD agencies that actively participate in biometric standards development within national and international standards organizations to facilitate DoD biometric interests. These standards organizations include InterNational Committee for Information Technology Standards (INCITS) M1, SC37, INCITS T4, and SC27. The working group also includes liaison representatives from non-DoD agencies such as National Institute of Standards and Technology (NIST) and National Biometric Security Project (NBSP).

In October 2003, the BMO coordinated with 20 DoD organizations to draft the DoD Biometric Standards Development Recommended Approach document. This document provides an approach to the identification of, participation in, and promotion of biometric standards within the DoD. Thanks to input received from DoD organizations, this document has been revised and updated to identify DoD-wide gaps. These gaps indicate a need for a DoD application profile, conformance testing standards, and conformance test suites.

The BMO is currently developing a DoD application profile standard entitled, "Biometric Profile-Interoperability and Data Interchange-DoD Implementations." Under development within INCITS M1, this application profile describes an infrastructure that supports a data collection system to capture biometric data from "Red Force" personnel. Red Force personnel are defined as detainees, civilian internees, enemy prisoners of war (EPW), and foreign persons of interest currently under U.S. Government control, or who are perceived as potential national security threats requiring further background investigation.

The following is the development timeline for this standard:

DOD APPLICATION PROFILE TIMELINE	
Project Proposal Submitted to INCITS M1	December 2003
Project Proposal Approved by INCITS M1	February 2004
First Draft Reviewed by INCITS M1 Working Group	May 2004
Second Draft Due	August 2004
Approved as Standard	2Q 2005

To address the gaps in conformance testing standards, the BMO is involved in a variety of efforts to develop such standards. For example, the BMO is serving as a co-editor for the draft International Organization for Standardization (ISO) standard "BioAPI Conformance Testing—Part 1: Methods and Procedures," which is being developed within SC37. Additionally, the BMO has proposed itself to SC37 as editor for the draft ISO standard "BioAPI Conformance Testing—Part 2: Test Assertions." Finally, the BMO is developing a BioAPI conformance test suite (CTS) following the methodologies outlined in these conformance testing standards. This CTS will allow the DoD to evaluate whether biometric products and system components conform to the BioAPI specification.

Policy development is also critical to allow the sharing of data within the DoD, the U.S. Government, and cooperating allies, as required. A significant step forward for biometric policy is the 02 February 2004 Assistant Secretary of Defense, Networks and Information Integration (ASD (NII)) memorandum, which requires DoD components to collect Red Force data following the FBI's Electronic Fingerprint

Transmission Specification (EFTS). The EFTS is critical to interoperability because it defines a common implementation of the ANSI/NIST-ITL 1-2000. Systems that are EFTS compliant are ANSI/NIST-ITL 1-2000 compliant. Furthermore, the EFTS defines the interface between the FBI's Integrated Automated Fingerprint Identification System (IAFIS) and other agencies' automated fingerprint identification systems.

In summary, a post-11 September 2001 paradigm shift is taking place within the U.S. Government due to the realization that biometric data must be leveraged to link individuals to previous names, aliases, and criminal or terrorist activities. For example, part of the information the military collects from Red Force personnel is biometric data. That data must be collected in such a way that it can be shared and searched by DoD and other U.S. Government agencies—requirements that demand the use of interoperable technologies. Standards are critical to such efforts and should be accompanied by policy that mandates the use of standards. This workshop series will facilitate increased collaboration among government agencies to leverage their resources to first make needed standards available and then implement their use to protect those serving on the front line.

DEPARTMENT OF HOMELAND SECURITY EXPERIENCE USING BIOMETRICS STANDARDS

Presenter: Brad Wing, Biometrics Coordinator, Department of Homeland Security (DHS) United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program

DHS Use of Biometrics

At the national level, DHS has regulatory mandates to use biometrics for border inspection, inspection of transportation workers, background checks, and the identification of applicants for citizenship and immigration benefits. For border inspection, DHS implemented the US-VISIT program on 05 January 2004. Under this program, when an individual applies for a visa at a Department of State consulate overseas, he or she is required to submit fingerprints and a facial photograph. When the individual attempts to enter the United States via a port of entry, a photograph and two fingerprints are captured by the inspector and compared against the fingerprint and photograph taken at the time of the visa application. This ensures that the individual entering the United States is the person who was granted the visa. Standards are critical to the success of this process because DHS wants to collect fingerprints and facial images that can be read, stored, and compared against criminal and terrorist watch lists in the future.

In addition to using biometrics in the identification of applicants for citizenship and immigration benefits, DHS has begun tracking asylum applicants. In the past, asylum applicants would send trained individuals, well versed in how to answer the application questions, in their place for interviews. This substitution increased the chances that the Department would approve an application. To avoid this ruse, DHS is working to collect biometric data at the time of the initial asylum application that can be used to confirm an individual's identity throughout the process—from the application to the interview to the application's approval.

Within DHS, Transportation Security Administration (TSA) has begun a pilot program instituting the use of biometrics in the identification of transportation workers. Workers will provide fingerprints and undergo background checks before being issued a Transportation Worker Identification Credential (TWIC). Biometric devices are then used to ensure that only the pre-screened, TWIC-carrying personnel enter restricted areas of transportation facilities.

DHS Roles and Responsibilities for Standards

The National Technology Transfer and Advancement Act requires the use of technical standards developed or adopted by voluntary consensus standards bodies. This means DHS can apply and enforce standards—once they are developed by groups such as the International Organization for Standardization (ISO) or InterNational Committee for Information Technology Standards (INCITS)—within the government.

At the international level, DHS is required to follow standards for travel documents established by International Civil Aviation Organization (ICAO), which is part of the United Nations. During the May 2004 ICAO meeting, the standards for the new electronic passports, "e-passports," were approved. An e-passport looks like a standard passport but contains an integrated circuit chip that stores an individual's identification information, including his or her biometric data. In the current implementation, the chip may only be written to once, and cannot be updated. However, the chip can be read from a proximity of 10 centimeters. Public Key Infrastructure and digital signatures have been adopted within the ICAO standards to ensure that authorized agents of the issuing nation wrote the information on each chip. ICAO has officially selected facial image as the default biometric for travel. However, at their option, nations can store fingerprint and iris information on the chips. As mandated by the Enhanced Border Security Act of 2002, DHS will require that nations participating in the visa waiver program issue passports following these standards. This is a very important step, as it ensures that biometric data will be consistent across all participating nations around the world. It also ensures that the data can be used, read, stored, and accessed in a consistent manner. Moreover, it does not tie users to a single vendor: the purpose of these standards is to enable many vendors to enter the market and allow different nations a choice of systems that will work together effectively.

Within the DHS organization, the DHS Chief Information Officer (CIO) is responsible for the development of information technology standards. The Under Secretary, DHS Science and Technology Directorate, has the responsibility of developing standards for emerging technologies. The DHS Biometrics Coordination Group is responsible for biometric standards development.

The DHS Biometrics Coordination Group is co-chaired by US-VISIT and DHS Science and Technology. This group represents multiple biometric disciplines from all DHS directorates (e.g., standards, policy, privacy, operational end users). This group:

- Coordinates DHS biometric technology policy and standards
- Identifies gaps in biometric policy and standards
- Reviews new DHS biometric technology projects
- Identifies common operational requirements and research objectives for DHS biometric systems
- Develops and communicates a unified DHS position on biometric issues to national and international standards organizations
- Coordinates information exchange and discussion of biometric issues with interagency community

DHS Experience Adopting Face Recognition Standards

DHS adopted the INCITS M1 draft standard, "Face Recognition Format for Data Interchange" (Draft ANSI INCITS 385) as the Department's standard, and developed a draft Facial Recognition Policy specifying the use of this standard for all DHS systems that store photographic data. This involved extracting and reordering portions of the standard to provide guidelines relevant to multiple DHS user groups (e.g., project managers, software system developers, and photographers and their subjects). Best

practices for producing uniform photographs and example photographs demonstrating compliance and non-compliance to the guidelines were extracted from the standard and included in the DHS policy.

The next steps with respect to the DHS Facial Recognition policy are to:

- Resolve issues with INCITS regarding copyright
- Finalize and issue the policy
- Communicate the policy to all affected parties
- Educate impacted parties on their roles in the implementation of the policy
- Analyze results of facial recognition prototype testing currently underway at the border
- Work with the DHS CIO's office to review proposals for new DHS projects employing facial recognition.

Overall, the exchange of data, information, and testing results requires collaboration. Fortunately, there seems to be a spirit of cooperation among the necessary parties, as evidenced by the turnout for this workshop. Future efforts for DHS biometric standards include development of policy for fingerprint matching systems, and coordination with the DHS procurement office to add biometric standards to the DHS standards inventory. The biometric test and evaluation methodologies, and test plans for DHS biometric systems have to be assessed. Best practices for biometric testing and reporting must be developed, and a test plan must be in place prior to implementing a biometric system.

PART II

AFTERNOON SESSION

OPEN DISCUSSION: BIOMETRIC APPLICATION, STANDARDS, AND GAPS

Moderator: Rick Lazarick, Department of Homeland Security (DHS)—Transportation Security Administration (TSA)

The purpose of this open discussion was to obtain specific information about a variety of biometric-related programs and projects currently in existence. Participants from the relevant agencies shared information regarding each program's target population, biometric modality, usage, and applicable standards. After this information was gathered, participants identified gaps that must be addressed in order to develop or accelerate standards. The discussion focused on the following programs:

- DHS –United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program
- DoD – Common Access Card (CAC)
- TSA – Transportation Worker Identification Credential (TWIC)
- DoD – Biometrics Automated Toolset (BAT)
- Intelligence Community – Watch Lists

While facilitating this information exchange, the moderator emphasized that once these questions are answered and the data is gathered, it must be carefully examined within and across the multiple programs. This will help identify the standards in development with time-critical, program schedule driven deadlines that need acceleration. Also, the moderator noted that the absence of necessary standards and gaps in current standards must be identified.

The following excerpts summarize the discussions of each program:

DHS—US-VISIT

Collection Population: Alien visa-holders and visa waiver travelers.

Modality: The US-VISIT program currently operates using biometric fingerprint data. Other considered methods, such as voice verification, were deemed too insecure after the terrorist attacks of 11 September 2001. Fingerprints are used in different ways depending upon the application within the broad border management application: some are rolled, some are flat, depending upon the operational necessities (e.g., time and processing, response time back). For example, Border Patrol takes 10-prints of individuals apprehended during illegal border crossings, to run a criminal background check through the FBI. Visa holders are enrolled in the system at the consulate. Currently, two flat prints are collected, but the plan is to eventually collect eight flats. Starting in October 2004, visa waiver travelers will have their fingerprints and photographs taken upon first entry to the United States—unlike visa holders, they will not be enrolled into the system prior to their arrival. The United States will rely

upon the biometric data that is stored in the passports. This means the United States will also rely on trusted governments to collect biometric information and digitally sign it to verify the authenticity of the biometric information contained in the passports.

Usage: Verification and validation.

Interoperability: DHS must have data that can be interchangeable and interoperable with:

- State Department: US-VISIT relies on the systems that collect biometric data from overseas consulates.
- Intelligence Agencies: US-VISIT must share biometric information with the intelligence agencies that manage terrorist and other watch lists.
- National Institute of Standards and Technology (NIST): US-VISIT relies on NIST because laws require the program to follow NIST recommendations on various standards and applications.
- Other Nations: US-VISIT must be interoperable with bi-national and multi-national organizations, and interoperable with the visa waiver nations, the U.N. and International Civil Aviation Organization (ICAO). The program must also deal with neighbors, Canada and Mexico, and ensure that the systems are compatible.

Standards Development Gap Action Issues: Currently, the US-VISIT program's fundamental profile and associated base standards are all fairly well developed for the modalities and for the border management application. The next step is to test whether private industry will be able to develop systems that comply with the standards and are truly interoperable. This includes testing whether the biometric data is useable and interoperable, and determining whether or not everyone is interpreting the standards in the same way.

Multi-Biometric Fusion: The DHS representative believes that a multi-biometric fusion standard application for the US-VISIT program will not be issued. This does not mean such an application would not be beneficial. The primary biometric for US-VISIT will be fingerprints verified upon entry. However, a standard operating procedure must be developed for individuals who do not have useable fingerprints. Also, watch lists must be considered. The Face Recognition Vendor Test (FRVT) 2002 showed that as the number of photos in a large gallery (group of photos used for comparison) increases, the number of possible matches also substantially increases. If additional biometric data were used, the number of responses could be filtered down, which in turn would decrease the number of referrals to secondary inspection.

DoD—CAC

Collection Population: Approximately 3.8 million military personnel including uniformed military, DoD civilians, and contractors.

Modality: Currently, when a CAC is issued, only the two index flat fingerprints are collected. The purpose of collecting this biometric is to authenticate the person should he or she "lock" his or her card

due to the three-time lockout mechanism. If a card is locked out, the individual must go back to the issuing station or use the recently developed CAC PIN reset system. Authenticating oneself with the fingerprint data will open the card again, and enable the user to perform various functions the CAC provides. DoD is considering associating a biometric with the CAC for transactional events, as an additional layer of security.

Usage: Identification as well as verification of military personnel for physical and logical access.

Applicable Standards: Since DoD implemented the CAC prior to the availability of standards, the two index fingerprints currently collected do not comply with any existing standard.

Interoperability: DoD has not made any formal decision as to whether or which biometrics will be stored on the CAC. Most of the interoperability issues that are being addressed are through the Government Smart Card Interoperability Specification (GSC-IS 2.1), which outlines how smart cards need to be configured for interoperability purposes. The next generation of the CAC—which features 64KB of storage, as opposed to the current 32KB of storage—will be issued beginning in December 2004, and should be GSC-IS 2.1 compliant, allowing interoperability from the smart card perspective.

Data Sharing: Due to the nature of sensitive information in the database, this system shares data with a limited number of other systems. However, it is predicted that standardization and interoperability will enable better data sharing.

Multi-Biometric Fusion: Currently, the only "multi-biometric" opportunity with the CAC is the possibility of reading both fingerprint images at the same time, as opposed to one at a time. In the future, other biometric capabilities could be recommended.

TSA—TWIC

Collection Population: Currently, TWIC is in pilot stage with an expected population of transportation workers who have identity badges that allow unescorted access to secure parts of airports and other transportation facilities. The TWIC issuance process involves the collection of 10 rolled fingerprints from the worker and a criminal background check that runs the fingerprints through the FBI's Integrated Automated Fingerprint Identification System (IAFIS) database (to determine if the worker has any prior arrests).

Modality: TWIC uses both reference and operational biometrics.

- Reference biometric: Everyone has the same sample taken; in this case, it will more than likely be fingerprints, though iris has also been considered. This biometric is used to prove identity when a worker picks up their card at a new facility or gets a replacement card.
- Operational biometric: Each facility can choose which biometric to use. This is an open structure. For example, San Francisco International Airport can continue to use its successful 12-year-old hand geometry system.

The goal is to have a single card that allows an employee with access rights to more than one facility to use a single credential and be enrolled in multiple operational biometric systems. At enrollment, pointers are written to each card. These pointers are notes that indicate that the individual has been enrolled in multiple transportation facility access control systems, and that they are authorized to use the local server and stored information to gain access to the desired facility.

Usage: The reference biometric is used for verification and identification. The operational biometric is used for verification.

Applicable Standards: All fingerprint, image, minutia, and pattern-based standards are applicable. The Transportation Workers Standard, an American National Standards Institute (ANSI) standard specifically designed for TWIC, should be completed by 4Q 2004.

Interoperability: TWIC will introduce the first prototypes in small pilot programs, and eventually expand to a wider user community. Interoperability is partly assured by the design of the system that stores the enrollment information and allows interoperability across facilities by programming the cards.

Data Sharing: Operational biometrics are stored locally by each transportation facility, and protected by data protection requirements. Reference biometrics are stored nationally, and are protected by the conventional data protection practices that are built into a wide system. There is some information exchange between agencies within the United States (between TSA and other airport authorities and law enforcement), but little international data sharing.

Multi-Biometric Applicability: Multi-biometric applicability is possible at either the operational level or the reference level; however the first prototype to be installed will most likely be a single biometric. As the program moves forward, there is nothing to prevent multi-biometric applications.

DoD—BAT

Collection Population: Enemy combatants, detainees, locally employed personnel, and HUMINT source ops. Red Force collection tries to address four categories with one system: (1) support to counter terrorism—identifying enemies or combatants, (2) detention operations—detainee management, (3) support to locally deployed personnel—foreign employees, (4) support to HUMINT operations.

Modality:

- Fingerprint is the primary modality because they are the most widely accepted and preferred. Originally, two index fingerprints were taken. DoD required compliance with a fingerprint standard announced in a memo issued by the ASD (NII) on 02 February 2004. At the detention center-level, Electronic Fingerprint Transmission Specification (EFTS)-compliant prints are collected from Red Force members. This method will eventually be implemented at the brigade level.
- Iris data has been collected from some detainees and has proven to be fairly accurate. This data can be cross-referenced with fingerprint data for further verification.

- Facial images are also being collected using face recognition algorithms. Initially, only one front-on picture was collected. Detainee booking stations now collect five photographs, including: both profiles, both 45-degree profiles, and a head-on view.
- BAT has the ability to collect and store voice files, and has collected voice files from some detainees. However, voice recognition has not yet been integrated because it is not mature enough to operate in the field.

Usage: Primarily enrollment. Identity authentication and verification are possible after enrollment has been implemented. All of the biometric information is stored locally in the in-theater database. If an individual is released and picked up again at a later date, the biometric data can be used to help identify them, ascertain where they were detained, who has talked to them, and what we know about them.

Applicable Standards: DoD has moved to the ANSI NIST/AFIS standards that the FBI uses. Eventually, brigades will implement these standards.

Interoperability: Initially, this technology was not interoperable between agencies because fingerprints were collected at different DPIs depending on the collecting agency. DoD has changed the standard that agencies follow in order to make the images interoperable. At the joint level, DoD and J-34 are working to ensure that the collection is to the standard.

Data Sharing: DoD does not currently have a policy on biometric information sharing with other U.S. Government agencies (outside of DoD). The representatives in the Office of the Secretary of Defense (OSD) are currently working on an information sharing policy to make sharing legal, but there are some concerns associated with this idea.

Action Items:

- Many agencies are going to the 500 DPI flat print scans. A workshop participant believes that the possibility of using the flat prints across more of the agencies should be addressed. This includes discussing the affordability, portability, and multi-biometric applicability of the 500 DPI finger print scanners.
- A workshop participant believes the increasing size of records has become an issue that needs to be addressed.
- A warfighter representative requested that DoD evaluate how much of the required data must be collected prior to prison detention in a tactical environment and how much of it can be collected once the detainees are brought back to the prison, thus lessening the burden on the military unit in the field.

Intelligence Community Watch Lists

Collection Population: Anyone who is on a terrorist watch list.

Modality: Any biometric within the Common Biometric Exchange Formats Framework (CBEFF). Since many different organizations have terrorist watch lists, and there is no standardization, these organizations must be ready to support the exchange of any modality.

Usage: The watch list can be used to transfer information about possible terrorists between different agencies and organizations.

Applicable Standards: CBEFF is the applicable standard. Most organizations that maintain terrorist watch lists that will be expected to conform to the CBEFF standard do not have much experience with the CBEFF standard. It is important that these watch lists are supported by the experts that are involved with this workshop, as well as in other environments, in order to ensure correct application of standards.

Interoperability: Interoperability is the primary goal for watch lists because it involves agencies sharing with whomever they choose.

Data Sharing: A complete record is not required for every watch list item. What is required is that any information that must be shared can be successfully exchanged. There are no policy statements concerning when, who, how, and where this data should be exchanged. All of these details need to be worked out independently, based on organizational needs, requirements, and legal constraints. Much of the time and effort required to build the standard metadata for each element has already been completed. The metadata for each element is information concerning where it was collected, who was the owner, which repository it came from, and its security classification handling information.

OPEN DISCUSSION: BIOMETRIC TESTING

Moderator: Mike Hogan, Standards Liaison for National Institute of Standards and Technology (NIST)'s Information Technology Laboratory (ITL)

During the "biometric testing" open discussion, participants shared information related to the biometric testing that their respective agencies are performing in the areas of conformity assessment, interoperability, performance, and security. The purpose of gathering this information is to eventually coordinate and leverage these activities across the government to reduce redundant efforts.

Biometric Testing and Conformity Assessment

Prior to beginning the discussion on biometric testing and conformity assessment, the moderator reviewed the following conformity assessment terms and definitions.

- Accreditation: Procedure by which an authoritative body gives formal recognition that a body or person is competent to carry out specific tasks.
- Certification: Procedure by which a third party gives written assurance that a product, process, or service conforms to specified requirements.
- Conformance Testing: Captures the technical description of a specification and measures whether an implementation faithfully implements the specification.
- Conformity Evaluation: Systematic examination of the extent to which a product, process, or service fulfills specified requirements.
- Conformity Testing: Conformity evaluation by means of testing
- Conformity: Fulfillment by a product, process, or service of specified requirements.
- Means of Testing: Hardware and/or software, and the procedures for its use, including the executable test suite itself, used to carry out the testing required.
- Reference Implementation: Implementation whose attributes and behavior are sufficiently defined by standard(s), tested by certifiable test method(s), and traceable to standard (s) that the implementation may be used for the assessment of a measurement method or the assignment of test method values.
- Test: Technical operation that consists of the determination of one or more characteristics of a given product, process, or service according to a specified procedure.
- Testing: Action of carrying out one or more tests.

Product developers have four testing options available for performing conformity assessment for their products:

- First-Party Testing: Product developers perform their own testing and then declare the products as conforming to certain standards.

- Second-Party Testing: Product developers have their products tested by a user-testing laboratory, which may be a U.S. Government agency.

- Third-Party Testing: Product developers have their products tested by an independent, accredited laboratory that is not controlled or influenced by the consumer. Although usually more expensive, products declaring conformity that have undergone third party testing are given more credibility from industry stakeholders.

- Product Test Results Sent to Validation/Certification Authority: The validation/certification authority examines the testing process used to validate the test results and verify that the product complies with the standard based on the test result. The validation/certification authority may issue a "Certificate of Validation" for consumers based on the testing results and established criteria for issuing the certificates. These criteria may include a percentage of tests the product must pass, and/or the tolerance range of allowable errors over one or several tests.

While discussing the biometric testing that their respective agencies are performing in the areas of conformity assessment, the participants addressed the following questions:

- Which agencies are currently performing or planning to perform biometric conformance testing?

- What standards are being used or will be used to perform biometric conformance testing?

- What test tools are being used or will be used to perform biometric conformance testing?

- Is there a need for testing laboratory accreditation?

- Is there a need for a testing certification body?

- Is there a need for a U.S. Government-wide conformity assessment program for biometrics?

In responding to these questions, a Department of Defense (DoD) Biometrics Management Office (BMO) representative noted that the DoD Biometrics Fusion Center (BFC)—the technical element of the BMO—leads biometric conformity assessment activities in DoD. The BFC has conformance testing underway for the BioAPI standard and is also developing finger imaging conformance testing. The representative noted that during the development of any base standard, a conformance testing standard must be developed concurrently to test whether products conform to that base standard. For example, currently there is a base American National Standards Institute (ANSI) standard called the BioAPI specification, version 1.1. A version of this standard is under development within SC37, the

international standards body on biometrics. For the conformance testing of this standard, the BMO is developing the draft International Organization for Standardization (ISO) standard entitled, "BioAPI Conformance Testing—Part 1: Methods and Procedures." The BMO has also submitted to SC37 a new work item for an ISO standard entitled, "BioAPI Conformance Testing—Part 2: Test Assertions."

A BMO representative also noted that there is a need for at least one laboratory that is an accredited testing laboratory. This laboratory should be created relatively soon because it would be responsible for performing conformance testing once the technology is available. Currently, the DoD BMO Biometric Standards Working Group is in the process of finalizing recommendations on a conformity assessment program. However, the DoD BMO Biometric Standards Working Group is not prepared to make a recommendation on how many laboratories are needed within DoD, or how responsibility should be divided between them. The BMO representative also noted that the DoD BMO Biometric Standards Working Group's opinion is that certification should be in place so that mutual recognition agreements (MRAs) can be established with other certified laboratories. This reduces testing redundancies as signees of MRAs agree to recognize the results of each other's testing, inspection, certification, or accreditation.

A Department of Homeland Security (DHS) representative noted that for access control technology, DHS would not set up its own testing facility. Instead, it relies upon other facilities for testing access control devices. Because of this, it is important that DHS have confidence that its access control technology has been properly tested to meet standards that are applicable for a particular application.

The DHS representative also noted that the law for e-passports states that DHS and the Department of State jointly determine whether a nation remains in the visa waiver program. This determination is based on whether the nation complies with International Civil Aviation Organization (ICAO) standards (these standards fold into the ISO biometric standards). In order to certify a nation's compliance, testing must be performed. Therefore, sample passports as well as live passports from these nations must be tested in order to verify that they can be used in an inspection environment. It is also important that U.S. travel documents are usable by other nations. It is for this reason that a joint international testing program is being established.

With regard to Transportation Worker Identification Credential (TWIC), the DHS representative noted that conformance testing must involve ensuring that airports are adequately installing, using, and implementing the biometric systems. With all of the other applications within the DHS, the question of which systems and what standards will be adopted remains unanswered and/or at the decision level. Finally, the DHS representative noted that the DHS Biometrics Coordination Group was established to address these very issues.

An Army CIO representative noted that the Common Criteria (CC) and National Information Assurance Partnership (NIAP) certification is a path for evaluation. This representative noted that an accreditation body for the Common Criteria laboratories does exist and there are approximately seven or eight accredited test laboratories at this point. Upon successful completion of any test, a product is awarded a certificate and the product's manufacturer is placed on validated product lists. Because NIAP certification is so difficult, certifications tend to be awarded to only small systems rather than large,

integrated systems. These large systems are certified using the DoD Information Technology Security Certification and Accreditation Process (DITSCAP), detailed in DoD Instruction 5200.40. The hope is that if the components of a larger system have been NIAP certified, the larger system will be able to go through the DITSCAP process much easier.

The Army CIO representative noted that the NIAP standards are written as a Protection Profile, which does not get vetted at national or international levels. In effect, the standards are actually the protection profiles and are statements of requirements of what the users want. Presently, no test tools have been certified against the protection profile. The NIAP laboratories are going to need assistance because most do not have experience testing biometric products. The Army CIO representative noted the need for laboratory accreditation and noted that a certification body within the NIAP program is currently responsible for laboratory accreditation. Finally, the Army CIO representative pointed out that there are Memorandums of Understandings established among government agencies in different countries to recognize and accept Common Criteria and NIAP certification.

National Biometric Security Project (NBSP) does not currently have any testing laboratories in operation. However, in establishing these laboratories, NBSP is following a mandate to sponsor, define, and conduct a technology test and evaluation program that is complementary to other federally sponsored testing and evaluation programs. This involves validating vendor performance claims, determining if technologies meet approved standards, and using testing and evaluation metrics and merits to achieve an acceptable and reasonable level of comparison considering variables (e.g., false match, false non-match). Finally, this mandate also directs the NBSP to conduct application and operational pilot testing and evaluation as required.

The Joint Staff (J-2) representative noted that the J-2 receives a large amount of feedback from the combatant commanders on biometrics. CENTCOM and the Army have worked diligently over the past six months to conform to the new DoD standard for fingerprints in a combat environment. The representative noted that standards should consider the end user, such as the combat forces, throughout the entire standards development process.

A NIST representative noted that NIST has had a conformance certification program in place for about eight years. This program is for the Wavelet Scalar Quantization (WSQ) compression algorithm used to compress fingerprint images that went into the FBI's standard entitled, "ANSI/NIST-ITL 1-2000, Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information." The certification testing for this specification is completed at the NIST laboratory. The two agencies that are involved are NIST and the FBI. The goal was to set up a system such that all images that came into the FBI would be readable by them, and those going out would be readable to the 50 states and other agencies. NIST is looking for WSQ compliance. WSQ is a standard that all agencies have used to compress fingerprint images, scanned to 500 pixels per inch. NIST used a reference implementation for vendors who were submitting their products to them. The two products were compared to determine whether the vendor's product was in compliance or not. This began in 1996 and these efforts have certified between 100 and 200 implementations.

Biometric Testing and Interoperability

The next portion of the biometric testing discussion focused on testing for interoperability. Participants discussed which agencies are currently conducting or planning to conduct biometric interoperability testing, and which biometric profiles are being used.

A NIST representative noted that an interoperability test that NIST is working with is the national standard, Finger Minutiae Data Interchange Format (ANSI INCITS 381-2004). NIST intends on substituting minutiae generated by the different vendors, as opposed to images, to determine whether NIST is able to get the same results and performance.

A Transportation Security Administration (TSA) representative noted that TSA plans to begin a test, conducted by the International Biometric Group, looking at interoperability of iris cameras. Three different devices will be tested using the format specified in the Iris Image Data Interchange Format (ANSI INCITS 379-2004). The ability to enroll and then verify across the different vendors will be studied. The vendors that will be tested will most likely be Oki, Panasonic and LG, each with their own camera sensor suite. Behind the hardware devices the common Iridian iris codes as well as the various logic associated with their proprietary method for matching will be used.

A Defense Information Systems Agency (DISA) representative noted that DISA is looking at incorporating BioAPI, which is in Joint Technical Architecture version 5.0, into the Common Operating Environment (COE). DISA will do this with hopes of eventually moving forward into the Network Centric Enterprise Services (NCES). DISA performed interchangeability testing between a BioAPI-compliant application and four different, specifically selected BioAPI-compliant technologies. Once these four technologies were selected, DISA performed testing to ensure the technologies would work properly with the BioAPI-compliant application, and then conducted individual tests. DISA also tested these technologies to see if they worked properly when multiple BioAPI technologies are installed on the same system at the same time in both a stand-alone and client-server implementation. This has been completed and DISA is now performing follow-on activities associated with these implementations.

Biometric Testing and Performance

The next portion of the discussion focused on biometric testing for performance. The moderator noted that standards projects that go the slowest—because they are the most difficult—are the performance testing and reporting standards.

During this discussion, the participants noted which agencies are currently engaged in, or are planning to conduct, biometric performance testing, and which biometrics are being tested.

Prior to beginning the discussion on performance testing, the moderator reviewed the following performance-related terms and definitions:

- Performance Testing: Measures the performance characteristics of an Implementation Under Test (IUT), such as its throughput and responsiveness, under various conditions.

- Biometric Performance Metrics: False Acceptance Rate (FAR), False Rejection Rate (FRR), False Match Rate (FMR), False Non-Match Rate (FNMR), Failure-to-Enroll (FTE), Failure-to-Acquire (FTA)

- Performance Reporting Mechanisms: Receiver Operator Curve, Detection Error Trade-off Curve (DET), Cumulative Match Curve (CMC)

- Reference Data: In information technology, reference data is any data used as a standard of evaluation for various attributes of performance.

According to a DHS representative, to judge biometric performance, projects should establish their goals and objectives before they begin collecting information. In doing this, however, projects must take into account measurements such as the amount of time it takes to collect a biometric from start to finish. For instance, at ports of entry, DHS considers when an inspection begins, how much time is related to the inspection's biometric collection process, and how much time is related to the transmission of the collected biometrics to a searchable database. To analyze the quality of the collected biometrics, DHS is sending the biometrics to NIST to determine whether the data collected is useful. DHS is doing this before the standards are actually in place.

A NIST support contractor noted that NIST recently completed a Fingerprint Vendor Technology Evaluation (FPVTE), which was an evaluation of 34 systems from 18 companies. Currently, the NIST legal department is reviewing the FPVTE prior to public release. The representative noted that there is a great deal of difficulty within the evaluation process. For example, some systems are highly sensitive to certain data types. The FPTVE involved 11 different data types provided by the Department of State, and five different sources within DHS, the FBI, and the State of Ohio. For example, the evaluation involved flat, rolled, and slap fingerprints. The evaluation also includes criminal, civil, and recidivist data. Any change to a variable within an evaluation affects the performance, however, the change affects each system differently. For example, some systems perform very well for certain data types while other systems cannot handle data that cannot be quantified as a quality measure. The representative also noted that evaluating tens of thousands or hundreds of thousands of records is a difficult process. The FPVTE involved fingerprint examiners working for several months for this single evaluation. One of the conclusions drawn from this evaluation is that examiners attempting to state error rates below 10^{-4} or 10^{-5} will call their credibility into question, since there is a great deal of doubt about how accurate these determinations can be.

The NIST support contractor noted that one could have data that is not operational fingerprint data that was very carefully collected. However, non-operational fingerprint data is usually pristine data. Performance testing using this non-operational data will be nothing like the testing results produced using operational data. The operational data obtained from a variety of places, such as Border Patrol, is rife with human error. Attempting to correct these human errors before, during, and after a performance test is a very difficult process and a large effort.

Following these comments, a workshop participant noted that the NIST support contractor touched on how important the quality of the biometric sample is—regardless of the type of biometric—to

determining how usable it is. The workshop participant noted that this is particularly important when dealing with criminal and terrorist watch lists. One may have to determine how useful a photograph could be in testing the performance of a system collecting facial biometrics. For example, a watch list may contain a facial image scanned from a foreign newspaper. The quality for this image is different than a standard passport photograph. In this scenario with this data type, how does one rate the quality of the photograph and its performance in a facial recognition system for a watch list application? To evaluate the photograph, one could consider whether the photograph was taken with a fish-eye lens. One could also consider the distortion of the lens itself and how that distortion affects the image.

A TSA representative noted progress at the international level regarding performance testing standards is developing at a rather high rate. Further, the standards organizations are developing definitions for metrics and reporting practices. However, once these definitions are established along with (to some extent) the method for conducting these tests, there are still many performance testing concerns to address. For example, the protocols for the performance testing must be determined. It also must be determined how to certify a product from a performance viewpoint rather than a pure conformance viewpoint.

The TSA representative also noted that the best performance testing for any product works best in scenario and/or operational testing. This representative noted that he has worked with an organization performing operational testing at airports for the past four years. He noted the results of these operational tests have been shared with stakeholders within the standards organizations. The TSA representative also noted that he believed federal agencies should update the performance testing work the U.K. National Physical Laboratory completed related to scenario testing. In fact, the TSA representative offered to champion a multi-agency, large-scale scenario test that that updates the principles established by the National Physical Laboratory and do a cross-modalities comparison test for access control-related applications of biometrics.

A NIST representative noted that in addition to the recent FPVTE, NIST has also completed some certification testing of a prototype of the Integrated Automated Fingerprint Identification System (IAFIS) used by the FBI. One of the main objectives of this testing was to determine the effect of using flat images. NIST found that you could use flat images without much loss in performance accuracy. The NIST representative also noted that NIST finished testing on the same type of equipment used by the DHS. These reports are available on the NIST website.

Biometric Testing and Security

Prior to beginning this discussion, the moderator noted that the work of InterNational Committee for Information Technology Standards (INCITS) T4, the national standards body for information technology security, includes biometric data protection techniques, biometric security testing, evaluations, and evaluations methodologies. The moderator also noted that SC27 is the international counterpart to INCITS T4.

A National Security Agency (NSA) representative, who is also the U.S. Head of Delegation to SC27, spoke on the security of biometric testing. This representative noted that during a recent SC27 meeting,

the standards body convened an ad-hoc meeting on biometrics. During this ad-hoc meeting, participants determined four agenda items, which were not all related to testing. These items are security management, biometric data authentication, biometric template protection, and security evaluation and testing. The representative noted that security evaluation and testing work has had a slow start because the original editor dropped out, forcing SC27 to identify a new editor. Finally, the representative noted her belief that SC27 needs to study the attributes of biometrics from a security perspective in order to assess what the vulnerabilities are and what the most cost effective route is to developing security standards for biometrics.

A BMO representative noted that security testing for biometrics is a gap that is in need of U.S. Government resources. This representative noted that the BMO participated in the recent INCITS T4 and SC27 meetings. However, there is little participation from other U.S. Government agencies. This representative also noted that the U.S. Government has the opportunity to take leadership roles in the area, but the agencies must show their commitment through providing editors or technical contributions for standards developed by INCITS T4 and SC27.

A DHS representative noted ISO's JTC 1/SC37 recently established a working group on biometrics and privacy. The DHS Privacy Office is the U.S. delegate to this committee.

The representative noted that in October 2003 the European Union issued a directive on biometrics, which is available on the European Union website. This directive notes rights related to the collection, storage, transmission and security of biometrics. This directive is why European Privacy Commissioners insisted on incorporating several security provisions for the storage of biometrics into the development of e-passport standards. For example, the European Privacy Commissioners insisted on the inclusion of an access control mechanism as a voluntary procedure within certain nations to prevent outsiders from illegally capturing data from e-passports. One such opportunity for unauthorized capture of e-passport information is eavesdropping on the transmission of data between the chip and the reader. German laboratory experiments have indicated this data transmission can be intercepted from up to 30 meters away.

The DHS representative noted that ICAO uses a four-tiered approach in the security of biometrics. First, digital signatures are used to ensure that the biometric data on the e-passport has been written by an authentic issuing agency. Optional access control measures include active authentication, which involves reading an item from inside the data page of the passport, and basic access control, which entails reading certain information and using that information as a key to open the data on the chip itself. In some cases, there is extended access control, which means that access to certain fields may be restricted outside the issuing nation. Beyond all these authentication levels, some nations may use encryption. For example, the Netherlands is planning to include fingerprint information on the country's passport chip. DHS will not have access to this chip because the Netherlands's constitution and protection laws require that the country ensure its chip is usable by local applications only.

Finally, the DHS representative noted that it is important that security and privacy be included in biometric applications in order to protect the data from being compromised.

APPENDIX A. WORKSHOP AGENDA

Agenda for the U.S. Government Workshop Biometric Standards in Support of the Global War on Terrorism 25 May 2004 • 0900 – 1630 Workshop Moderator: MAJ Dupont, Army PM SET-D		
Time	**Item**	**Moderator / Speaker**
0830 – 0900	Registration	—
0900 – 0915	Opening Remarks	Priscilla Guthrie Deputy Assistant Secretary of Defense Deputy CIO
0915 – 0935	Biometric Standards Overview	Fernando Podio National Institute of Standards and Technology
0935 – 1015	Biometric Standards in Support of the Global War on Terrorism: A Department of Defense Perspective	John D. Woodward, Jr. Department of Defense
1015 – 1045	Break	—
1045 – 1130	DHS Experience Using Biometric Standards	Brad Wing Department of Homeland Security US-VISIT Program
1130 – 1300	Lunch	—
1300 – 1415	Biometric Application, Standards, and Gap Identification	Moderator: Rick Lazarick Transportation Security Administration / Department of Homeland Security
1415 – 1445	Break	—
1445 – 1600	Biometric Testing	Moderator: Mike Hogan National Institute of Standards and Technology
1600 – 1630	Conclusions and Future Action Items	John D. Woodward, Jr. Department of Defense

APPENDIX B. PRESENTER BIOGRAPHIES

Priscilla Guthrie became the Deputy Assistant Secretary of Defense (Deputy Chief Information Officer) in December of 2001. She serves as principal adviser to the Department of Defense Chief Information Officer, DoD-CIO, on the integration of principles of information management and technology into all Department functional activities. Her responsibilities include implementation of the Klinger-Cohen Act of 1996 and Title X Requirements for interoperability across the Department. She provides leadership for integration of the Department's information systems and services into an enterprise-wide global information grid, encompassing the collection, generation, storage, display, and protection of information Department-wide. Ms. Guthrie's primary goal during her tenure is to achieve network-centricity across the Department. She plans to set priorities to enable, develop, and implement network-centric concepts and capabilities, and establish specific goals and measures to demonstrate progress.

Ms. Guthrie came to DoD after a career in IT, automotive, and government business. Most recently, she served as Vice President of E-business for TRW Incorporated. She reported to the Chairman/CEO, and was responsible for developing and directing the global e-business strategy. Prior to this, Ms. Guthrie was Vice President and General Manager of TRW Systems. Her organization provided information technology-based business solutions and services to a worldwide client base.

Ms. Guthrie earned a Bachelor of Science degree in electrical engineering from Pennsylvania State University and a Master's degree in business administration from Marymount University.

Fernando L. Podio is a member of the Computer Security Division of the Information Technology Laboratory at the National Institute of Standards and Technology (NIST). Mr. Podio has worked at NIST since 1983. He has been involved in different aspects of IT development, measurements, and standards for over twenty-five years.

For the past five years he has been involved in biometric research and standardization. He is currently responsible for the NIST program on accelerating the development of biometric standards and associated conformity assessment activities for Homeland Security and the prevention of ID theft. Before his work in biometrics began, he conducted research and testing of intelligent data storage devices, sequential data storage media and optical digital data disks. He chairs the InterNational Committee for Information Technology Standards (INCITS) Technical Committee M1, Biometrics, and is the Chairman of ISO/IEC Joint Technical Committee 1 (JTC 1) Subcommittee 37 (SC 37) - Biometrics.

Mr. Podio also co-chairs the Biometric Consortium. He has shared a 2003 Group U.S. Department of Commerce Gold Medal Award and the InterNational Committee for IT Standards Gene Milligan Award in recognition of his leadership work in biometric standards. His involvement in biometric also led to two other awards, NIST's 2000 William P. Slichter Award for "Outstanding Achievement in building or strengthening ties between NIST and industry" and a Federal Laboratory Consortium for Technology Transfer award for technology transfer of biometric specifications to industry.

John D. Woodward, Jr. is the Director of the Department of Defense Biometrics Management Office. Mr. Woodward comes to the Department from the RAND Corporation under the authority of the Intergovernmental Personnel Act, which permits movement of personnel between qualifying organizations. At RAND, he served as a senior policy analyst working on national security, intelligence, and technology policy issues.

Mr. Woodward's particular area of interest is biometrics. He has testified about biometrics before Congress, the Commission on Online Child Protection, and the Virginia State Crime Commission. His publications on the subject have appeared in *Government Computer News, Legal Times, Pittsburgh Post-Gazette, Proceedings of the IEEE, United States Law Week, University of Pittsburgh Law Review, Washington Post*, and others. He is the primary author of *Biometrics: Identity Assurance in the Information Age*, McGraw-Hill, 2003.

Prior to joining RAND full-time in 2000, Mr. Woodward served as an Operations Officer for the Central Intelligence Agency for twelve years.

A member of the Virginia State Bar, Mr. Woodward received his Juris Doctor degree magna cum laude from Georgetown University Law Center in Washington, D.C. He was a Thouron Scholar at the London School of Economics, University of London, where he received his M.S. in Economics. He received his B.S. in Economics from the Wharton School of the University of Pennsylvania.

Brad Wing works for the U.S. Department of Homeland Security (DHS), serving as Biometrics Coordinator in the US-VISIT Program. He has been actively involved in the use of biometrics in immigration related applications for many years, and is now co-chair of the DHS Biometrics Committee. He serves as chair of the Cross Jurisdictional and Societal Issues Working Group of M1, the U.S. committee for biometrics that represents the U.S. in the International Organization for Standardization (ISO). He also serves on the New Technologies Working Group of the International Civil Aviation Organization (ICAO).

Rick Lazarick, an engineer with U.S. Department of Homeland Security, Transportation Security Administration (TSA) Research and Development for 6 years, specializes in technologies applicable to airport physical security, biometrics, access control and analysis of security system effectiveness. He has over 30 years of experience in the aviation industry, in both the federal government and other industries of the federal government.

Mr. Lazarick is currently the TSA Program Manager for Biometrics and Access Control R&D and is the DHS voting member on InterNational Committee for Information Technology Standards (INCITS) Technical Committee M1 – Biometrics. He is also Chairman of the M1 Ad Hoc Group for Evaluating Multi-biometric Systems and is a member of the U.S. Delegation to the international ISO/IEC SC37

subcommittee on Biometrics Standards. He co-chaired the Aviation Security Biometrics Working Group, which published its findings November 2001.

Previously, Mr. Lazarick was instrumental in the development of the FAA's "Total Architecture for Aviation Security" which was based on an effectiveness analysis method of his design.

Mr. Lazarick received a B.S. degree in Aerospace Engineering from Brown University in 1971, and an M.A. degree in Mathematics from The College of New Jersey.

Michael D. Hogan is responsible for liaison with the voluntary standards community for the Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST). He represents NIST at national and international voluntary standards organizations that manage the development of standards and associated testing methodologies for information technology (IT), and he participates in the development of policies on standards and conformity assessment issues. Mr. Hogan is presently serving as the NIST member of the Executive Board of the InterNational Committee for Information Technology Standards (INCITS) and as a NIST representative to INCITS Technical Committee M1 -- Biometrics. In September 2003, Mr. Hogan was appointed the Working Group Convener for ISO/IEC JTC 1/SC37 WG 4 - Biometric Functional Architecture and Related Profiles.

From 1982 to 1987, he managed the NIST Computer Storage Media Group, which conducted research in methods to characterize and measure magnetic and optical digital data storage media. In previous positions at NIST, he developed reference measurement services and data interchange standards for computer storage media. An electronics engineer, Mr. Hogan has worked at the National Institute of Standards and Technology (formerly National Bureau of Standards) since June 1974.

APPENDIX C. ORGANIZATIONS REPRESENTED

WORKSHOP PARTICIPATING ORGANIZATIONS	
Headquarters U.S. Army Deputy Chief of Staff for Intelligence (Army G-2)	National Detainee Reporting Center (NDRC)
Army Intelligence Center	National Biometric Security Project (NBSP)
Product Manager, Secure Electronic Transactions—Devices (Army PM SET-D)	National Institute of Standards and Technology (NIST)
U.S. Army Training and Doctrine Command (TRADOC)	National Security Agency (NSA)
Central Intelligence Agency (CIA)	Office of Management and Budget (OMB)
Department of Homeland Security (DHS)	Office of the Secretary of Defense (Acquisition Technology and Logistics) (OSD/AT&L)
Defense Information Systems Agency (DISA)	Office of the Secretary of Defense (Networks & Information Integration) (OSD/NII)
Defense Manpower Data Center (DMDC)	Office of the Secretary of Defense (Policy) (OSD/P)
DoD Biometrics	Department of State
Department of Justice (DoJ)	U.S. Navy
Federal Bureau of Investigation (FBI)	Headquarters United States Air Force, Directorate of Command, Control, Communications & Computers, Intelligence, Surveillance & Reconnaissance (C4ISR) (USAF/XIC)
Intelligence Technology Information Center (ITIC)	U.S. Central Command (CENTCOM)
Joint Chiefs of Staff Director for Intelligence (JCS/J-2)	U.S. Customs Service
Joint Chiefs of Staff Director for Operations (JCS/J-3)	U.S. Marine Corps

APPENDIX D: ABBREVIATIONS AND ACRONYMS LIST

ABBREVIATIONS/ ACRONYMS	DEFINITION
ANSI	American National Standards Institute
ASD (NII)	Assistant Secretary of Defense, Network and Information Integration
BFC	Biometrics Fusion Center
BioAPI	Biometric Application Programming Interface
BMO	Biometrics Management Office
CBEFF	Common Biometric Exchange Formats Framework
COTS	Commercial-Off-The-Shelf
CTS	Conformance Test Suite
DHS	Department of Homeland Security
DoD	Department of Defense
EFTS	Electronic Fingerprint Transmission Specification
FPVTE	Fingerprint Vendor Technology Evaluation
IAFIS	Integrated Automated Fingerprint Identification System
ICAO	International Civil Aviation Organization
INCITS	InterNational Committee for Information Technology Standards
INCITS M1	National Standards Body for Biometrics
INCITS T4	National Standards Body for Information Technology Security
ISO	International Organization for Standardization
ITL	Information Technology Laboratory
NBSP	National Biometric Security Project
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
NSA	National Security Agency
OSD	Office of the Secretary of Defense
SC 37	International Standards Body for Biometrics
SMT	Scar Mark & Tattoo
TSA	Transportation Security Administration
TWIC	Transportation Worker Identification Credential